



National Infrastructure Protection Center NIPC Daily Open Source Report for 21 January 2003

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- U.S. Newswire reports Interior's Assistant Secretary for Land and Minerals Management delivered to Congress a study of U.S. oil and gas resources in five western basins. (See item [2](#))
- HealthNews.Co reports that researchers have developed a test for plague that could help save lives in the event of a bioterrorist attack. (See item [19](#))
- The Washington Times reports that two al Qaeda suspects were taken into custody as they tried to enter the United States after their fingerprints were matched with ones lifted by U.S. military officials from documents found in caves in Afghanistan. (See item [23](#))
- CNET News reports the Department of Defense is concerned that too much unclassified but "worrisome" material is on the Web, and that controls over what is posted need to be tightened. (See item [27](#))
- The Boston Globe reports the engineering journal IEEE Security and Privacy notes discarded hard drives were found full of personal data. (See item [29](#))

NIPC Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [NIPC Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *January 17, Platts Global News* — Venezuelan oil strike has cut 400,000 b/d from capacity. Venezuela's ongoing national oil strike has reduced the country's production capacity by

a permanent 400,000 b/d to some 2.35–mil b/d, the International Energy Agency said Friday. It said the shutting in of wells, which began Dec 2, will have damaged some of Venezuela's low–pressure oilfields. Other oilfields would take "months not weeks" to restart after the strike ends, the IEA said in its latest monthly report. "The loss from well shut–ins may be even deeper if the current shutdown lasts much longer," the agency said. It said the strike, which took 1.95–mil b/d of production offline in December, remains "troubling and uncertain" to world oil markets.

Source: <http://www.platts.com/stories/oil2.html>

2. *January 16, U.S. Newswire* — **Interagency study of oil, gas resources in five U.S. basins issued; Study fulfills obligation of act signed by Clinton Administration.** Interior's Assistant Secretary for Land and Minerals Management Rebecca Watson today delivered to the Congress a study of U.S. oil and gas resources in five western basins. The interagency scientific inventory was prepared at the request of Congress under the provisions of the 2000 Energy Policy and Conservation Act. Under the Act (P.L.106–469), signed into law by former President Clinton, federal agencies are tasked with developing a national inventory of all oil and gas resources and reserves beneath federal lands. The report released today is the first study designed to fulfill this obligation. Additional studies will be initiated to inventory oil and gas beyond the areas studied in the report that Watson released today. **The report, entitled "Scientific Inventory of Onshore Federal Lands Oil and Gas Resources and Reserves and the Extent and Nature of Restrictions or Impediments to Their Development," evaluates the five areas in the West that contain the bulk of the natural gas and much of the oil resources under federal ownership in the onshore United States. It examined energy resources located in five major geologic basins in the interior West: the Paradox/San Juan Basins in Colorado, Utah and New Mexico; the Uinta/Piceance Basins in Colorado and Utah; the Greater Green River Basin in Wyoming, Colorado and Utah; the Powder River Basin in Montana and Wyoming; and the Montana Thrust Belt in Montana.** "This report represents the first time Congress has asked for a study that provides not only an estimate of oil and gas resources and reserves, but also information on any constraints that may limit development of these energy resources," Watson said. "This inventory is not a decision–making document. It is a planning tool for the Congress that identifies areas of high and low oil and gas potential and the nature of constraints to the development of those resources in the basins in the interior West." **The report provides estimates of oil and gas resources and reserves beneath the five basins and an inventory of the extent and nature of limitations to development. The report does not make any policy recommendations in response to its findings.** The oil and gas figures are based on U.S. Geological Survey's undiscovered technically recoverable–resource estimates and the Energy Information Administration's proved–reserve calculations. The key findings of the inventory are as follows: An estimated 57 percent of oil and 63 percent of gas are available under standard stipulations, and only 15 percent of oil and 12 percent of gas are totally unavailable. The remaining oil and gas are available with increasing restrictions on development. Land that is closed to development contains comparatively little oil and gas potential. Note: Copies of the report can be obtained by writing to the Bureau of Land Management, Office of Public Affairs, 1849 C Street, N.W., MS–LS 406, Washington, D.C. 20240. The report is also available on the Internet at <http://www.doi.gov>.
Source: http://www.energycentral.com/sections/gasnews/gn_article.cfm?id=3 576004

3. *January 16, Associated Press* — **Nuke plant fire leads to reactor shutdown.** A transformer fire at a nuclear plant injured a security officer and led to the automatic shutdown of one of the plant's two reactors. **The fire Wednesday night at the Donald C. Cook Nuclear Plant in southwest Michigan also resulted in a brief activation of the site's emergency plan, the plant's owner, American Electric Power Co., said in a news release.** A security officer was treated for smoke inhalation. The transformer, which is outdoors and adjacent to the plant, is used to increase the voltage of the plant's generator for more efficient long-distance transmission of electricity. **When the transformer failed, the plant's operating system automatically shut down the Unit 1 reactor, which was operating at full power. All safety systems responded appropriately, and the reactor was not damaged, AEP said. The plant's fire brigade extinguished the fire in 35 minutes, and the plant notified the Nuclear Regulatory Commission and state and local emergency-response agencies, AEP said. The fire's cause remained under investigation.**

Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id=3576006

[\[Return to top\]](#)

Chemical Sector

4. *January 16, Government Executive Magazine* — **Senator reintroduces chemical plant security.** Sen. Jon Corzine, D-N.J., reintroduced legislation Tuesday to increase security at U.S. chemical plants to reduce the threat of an intentional release of toxic chemicals through a terrorist attack. The Senate Environment and Public Works Committee had approved the proposed Chemical Security Act unanimously in late July, but the full Senate failed to act before the congressional session ended, according to Corzine spokesman Darius Goore. The bill has been reintroduced in the new Congress with only a few technical changes, such as replacing references to the Office of Homeland Security with the term "Homeland Security Department" Goore said, adding that no hearings on the bill are scheduled yet. **The bill would require the Environmental Protection Agency and Homeland Security Department to identify high-priority chemical plants based on the chemicals they produce or store and their proximity to populated areas. Once such plants have been identified, the two agencies would be required to craft regulations requiring the plants to develop vulnerability assessments and implement response plans.** Plants would have up to year after the regulations, release to develop vulnerability assessments and up to 18 months to develop their response plans. The bill envisions chemical plants working with local law enforcement and first responder units to develop vulnerability assessments and response plans, which would then be submitted to the two agencies for review. The EPA and Homeland Security Department could issue orders to correct any deficiencies and to impose fines and penalties on plants that failed to comply. **The bill also seeks to prevent terrorists from obtaining information on a chemical plant that could be useful when planning an attack.** A plant's vulnerability assessment and response plan would not be made publicly available. Instead, only information on the EPA and Homeland Security's certification of those plans would be available for public review.

Source: <http://www.govexec.com/dailyfed/0103/011603gsn1.htm>

5. *January 16, BBC News* — **Italy seizes suspicious chemicals.** Police in Italy have seized 50 metric tons of industrial chemicals bound for Libya, on suspicion that they might be used to

make weapons of mass destruction. **The chemical, identified as morphaline, is used in resins and solvents, but is also on a United Nations black-list of materials as it could be used to produce chemical weapons.**

An Italian newspaper said the chemicals were a compound of mustard gas. But Italian prosecutors did not comment on the report, saying only that the cargo had dual use. "The seized substance could be used to make chemical weapons, but can also be used to clean and lubricate oil drilling equipment," prosecutor Francesco Lalla told Reuters news agency.

Source: <http://news.bbc.co.uk/2/hi/europe/2666781.stm>

[[Return to top](#)]

Defense Industrial Base Sector

6. *January 20, New York Times* — **U.S. says it is better prepared to ship arms and equipment to Gulf.** The United States is much better positioned now than it was during the buildup for the 1991 Persian Gulf war to move forces and matériel quickly and smoothly to the region, military logisticians say. A decade ago, the Navy's Military Sealift Command had only 24 pre-positioned ships and 8 faster sealift ships to use in a crisis. Nagging problems with its cargo ships forced the Navy to charter scores of foreign vessels to help carry thousands of tons of supplies to Saudi Arabia. **Since 1992, the Sealift Command has invested more than \$5 billion to buy a fleet of ocean freighters, and the military has positioned huge stocks of weaponry and supplies for the Army, Air Force and Marine Corps aboard ships in the Indian Ocean and Mediterranean Sea and in warehouses in allied gulf states.** Today, the Sealift Command has 42 pre-positioned ships, 8 fast sealift ships and 10 so-called roll-on, roll-off vessels, the most efficient ships for transporting tanks, armored personnel carriers and other vehicles. **After the terrorist attacks of Sept. 11, 2001, the Sealift Command took several steps to protect the fleet against strikes at sea. The command hired a Navy criminal investigator to help integrate the intelligence databases of the Coast Guard and Federal Bureau of Investigation into the command's systems. Crew members on all ships carrying American military cargo are now vetted. So far, about a dozen of the 4,000 seamen screened have shown up on watch lists monitored by law enforcement officials, and were removed from the crews before their ships sailed, said Vice Adm. David L. Brewer III, leader of the Sealift Command. Many ships now carry armed military security teams for added protection. "We put teams on ships based on the cargo," Admiral Brewer said, citing weaponry and ammunition as among the most delicate cargoes.**

Source: <http://www.nytimes.com/2003/01/20/politics/20SEAL.html>

7. *January 17, New York Times* — **Pentagon draws up a 20-to-30-year anti-terror plan.** The nation's top military officer has approved and sent to the armed services and the Pentagon's worldwide commands a comprehensive plan to combat terror that includes confronting countries that sponsor terrorism, senior defense officials say. **The 150-page classified document, called the National Military Strategic Plan for the War on Terrorism, provides the first long-term, strategic framework for the military on how to carry out its portion of the campaign against terror, according to officials familiar with the plan.** It is meant to complement similar counterterrorism strategies developed by the State Department, Central Intelligence Agency, Federal Bureau of Investigation and other government agencies. **Approved in October by Gen. Richard B. Myers, the chairman of the Joint Chiefs of Staff,**

the document outlines an approach that aims to disrupt and destroy terrorist organizations like Al Qaeda, and confront countries and organizations that sponsor or support terrorism. The plan also describes a long-term goal of creating a global environment that would be hostile to terrorism, the officials said.

Source: <http://www.nytimes.com/2003/01/17/politics/17STRA.html>

[[Return to top](#)]

Banking and Finance Sector

8. *January 20, New York Times* — **\$3 million U.S. computer theft.** Last month, Pakistani and American investigators arrested Khurram Iftikhar, a 25-year-old Pakistani college dropout. **The case, investigators say, demonstrates the increasing sophistication of Internet surveillance technology by investigators and the global reach of online fraud.** From the comfort of his home and office in Karachi, investigators say, Mr. Iftikhar stole more than \$3 million worth of computer equipment. He did it using keystrokes, mouse clicks, phone calls and faxes, as well as occasional two-hour flights to nearby Dubai. There, he rented an apartment, bought a BMW and occasionally paid Federal Express, one of many American companies he is accused of duping. **The investigators said Mr. Iftikhar used the same technique over and over. First, he offered a piece of computer equipment for auction on E-Bay or Yahoo. Bids poured in, and a winner was declared. Mr. Iftikhar collected the successful bidder's credit card information and address but never sent the equipment. Armed with valid credit card numbers, the investigators say, he logged on to the Web sites of Dell, Compaq, Gateway, Hewlett-Packard and Office Depot, among others, and bought computers, monitors and other equipment. He had the companies ship the goods to Mail Boxes Etc. in the United States and Canada, where he had rented mailboxes online under false names.** After delivery, he would ask Federal Express to ship the equipment to Singapore, where a shipping company forwarded it to Dubai. From there, it was shipped on to Karachi and sold by Mr. Iftikhar's company as legitimate merchandise.

Source: <http://www.nytimes.com/2003/01/20/international/asia/20KARA.html>

9. *January 17, New York Times* — **Big Puerto Rico bank settles U.S. money laundering case.** The Justice Department said today that Banco Popular de Puerto Rico, the island's largest bank and a company with a major presence in the continental United States, would pay \$21.6 million in penalties to settle accusations that it laundered millions of dollars in drug money. **Under the agreement, the bank will avoid criminal prosecution.** The deposits, totaling \$20 million, were often brought to the Old San Juan branch of the bank in "paper bags or gym bags filled with small-denomination bills" from June 1995 to September 1998, legal papers said. **Banco Popular, which is based in San Juan and has 100 branches in the United States and 200 in Puerto Rico, admitted that it did not file the "suspicious activity" reports required by federal antilaunching rules, or filed untimely or inaccurate reports, investigators said.** "Banks are our first defense against money launderers, drug dealers and even terrorists who would attempt to abuse our financial institutions," said Michael Chertoff, an assistant attorney general who heads the Justice Department's criminal division. "Today's agreement recognizes that Banco Popular has been forthright in accepting its responsibility."

Source: <http://www.nytimes.com/2003/01/17/business/worldbusiness/17LAUN.html>

Transportation Sector

10. *January 17, Atlanta Business Chronicle* — **U.S. DOT approves Delta alliance with Northwest, Continental. The U.S. Department of Transportation (DOT) has approved Delta Air Lines Inc.'s long awaited codeshare agreement with Northwest Airlines and Continental Airlines, the government said January 17.** The agreement, which Atlanta-based Delta first applied for in August 2002, will bring Delta some needed revenue this year as the carrier expects more bad quarters ahead. The government allowed a similar agreement between United Airlines and US Airways to take effect on October 2. **The codeshare agreement would allow the carriers to place their designator codes on each other's flights in most markets and will allow the three carriers to sell seats on each other's flights — with some limitations the government outlined.** DOT officials said they struck a middle ground that was both favorable to consumers and allowed the alliance carriers to enjoy increased efficiencies. Under the DOT provisions, the three carriers would have to make surplus airport gates available to other carriers, and 60 percent of any new code-sharing flights resulting from the alliance would have to be operated to unserved, underserved or smaller communities. **To maintain competition, DOT said the carriers may not coordinate or agree among themselves on matters such as fares, route entry or exit, or capacity.**

Source: <http://atlanta.bizjournals.com/atlanta/stories/2003/01/13/daily51.html>

11. *January 17, Associated Press* — **Court mandates study Mexican trucks' impact. A federal appeals court Thursday ordered the U.S. government to study the potential environmental effects of reopening U.S. highways to Mexican trucks for the first time in two decades.** The decision by the 9th U.S. Circuit Court of Appeals came after environmental, labor and trucking industry groups challenged a November order by President Bush opening the roads. Charles Miller, a Justice Department spokesman, said the government was reviewing the decision and had not decided whether to appeal. **Since 1982, trucks from Mexico had been allowed only in 20-mile commercial border zones, where Mexican rigs had to transfer their cargo to U.S. trucks that then made deliveries within the United States.** After Bush's order, the Transportation Department received numerous applications from Mexican carriers and bus companies, but none of their vehicles has yet to begin traveling on U.S. highways.

Source: <http://www.bayarea.com/mld/mercurynews/business/4968903.htm>

Postal and Shipping Sector

12. *January 17, Shipping Times* — **'Comply with advance cargo manifest rule': February 2 deadline won't be extended, says World Shipping Council. The World Shipping Council (WSC) has strongly urged all shipping lines and shippers to be prepared to fully comply with U.S. Customs' 24-hour advance cargo declaration requirements from the February 2 deadline.** Advising its members that no grace period can be expected, and warning that enforcement will apply to all U.S.-bound voyages beginning from February, WSC said the 'potential consequences for non-compliance with these new rules are obviously very

substantial.' They include fines, no-load orders and the possible denial of unloading non-compliant containers in the U.S.

Source: <http://business-times.asia1.com.sg/sub/shippingtimes/story/0.4574.69951.00.html?>

13. *January 17, Shipping Times* — **Malaysia ready to sign onto US box screening initiative. Malaysia has 'no problems' signing onto the US Customs Container Security Initiative (CSI), despite an earlier lukewarm response, according to Malaysia's Ministry of Transport.** A senior Malaysian official told Shipping Times he had little doubt Malaysia's ports would join the box pre-screening and customs exchange program within months. Once scanned and checked locally, containers will no longer have to undergo the same procedure at US ports, Malaysian Transport Minister Ling Liong Sik said, avoiding unnecessary scrutiny of Malaysian cargo. Designed to detect and pre-screen high risk container cargo before it departs for US ports, CSI involves stationing US Customs officers at foreign ports and sharing information on suspect cargo internationally. **CSI initially targeted the world's top 20 ports, which did not include Malaysia, but growing numbers of transshipment boxes at Malaysian ports prompted the US to also seek the country's participation.**

Source: <http://business-times.asia1.com.sg/sub/shippingtimes/story/0.4574.69950.00.html?>

14. *January 17, Associated Press* — **Ports start using secure-container system. Eleven of the world's busiest seaports have started using an electronic container security system that was developed to help the U.S. military keep track of food, ammunition and other gear shipped overseas. The technology relies on electronic seals placed on container closures.** Using radio signals, the seals can transmit information about where the container is, what is inside it and whether it has been opened – all crucial in thwarting smugglers or terrorists. Several million cargo containers – about 95 percent of U.S. international trade – enter the United States every year through its 361 sea and river ports. **Since Sept. 11, many people have worried that terrorists might use the 40-foot containers to sneak biological weapons or other arms into the country.**

Source: http://story.news.yahoo.com/news?tmpl=storyp_on_re_us/port_security_1

15. *January 17, Associated Press* — **Strike paralyzes ports in several EU nations. Port workers in several European Union nations went on strike Friday to protest EU liberalization plans which they fear would cut their pay, diminish the quality of services and severely hamper port safety.** Workers blocked the entry to all ports in Finland and Belgium and partially closed down the German ports of Hamburg and Bremerhaven, said Eduardo Chagas, the political secretary of the European Transport Workers' Federation in an initial report. Labor action in the Netherlands slowed down work in the world's biggest port, Rotterdam, and closed down the Amsterdam port and facilities in the southern Netherlands. Chagas said protesters affected work in French and Spanish ports as well.

Source: http://story.news.yahoo.com/news?tmpl=storyp_wo_en_po/eu_gen_eu_port_strike_1

[[Return to top](#)]

Agriculture Sector

16. *January 17, Wisconsin Ag Connection* — **Newcastle disease spreads to Nevada poultry. Exotic Newcastle Disease has apparently spread to poultry in Nevada. It was detected in a**

backyard poultry flock in Las Vegas, a spokesman for the Nevada Department of Agriculture said Thursday. U.S. Agriculture Department and state officials were working on a surveillance program to test the flocks in the area for the disease, including about a dozen commercial poultry operations nearby, said Ed Foster, a spokesman for the state agriculture department. An immediate quarantine was imposed in Clark County, which includes Las Vegas, and Nye County, Foster said.

Source: <http://www.wisconsinagconnection.com/story-national.cfm?Id=712003>

17. *January 17, Associated Press* — **Midwest, Western cattle ranchers worried about drought. The drought that has parched large stretches of the northern and central Plains, Rockies and spots in the Midwest has forced many ranchers to sell all or parts of their herds as rangeland has dried up and hay prices have escalated.** Others have shipped their animals out of state to feed in greener pastures. Neither industry nor government officials know how many ranchers have quit or what the dollar losses are. But all agree the situation is dire. "Frankly, I'm a lot more worried now than I was a year ago," Wythe Willey, president of the National Cattlemen's Beef Association, said. **Wyoming agriculture officials estimate about 35 percent of the state's roughly 1.5 million herd was sold last year because of the drought. The Montana Department of Livestock estimates the state's herd of 2.8 million cattle has been reduced by 250,000 to 300,000. In east-central Nebraska, some ranchers have cut their herds by 25 and 30 percent as rangeland has withered and wells have gone dry. South Dakota Agriculture Secretary Larry Gabriel said ranchers in the western half of the state sold or were considering selling up to 50 percent of all the cattle.** Statewide, about 20 percent of the 1.85 million cattle may have been sold. Colorado Agriculture Commissioner Don Ament said he believes only a few of the state's herds have been liquidated. Many more, however, have been reduced. "We've lost substantial," Ament said. "We think worst-case scenario that we may have lost a million, which is probably a third of Colorado's numbers."

Source: http://www.trib.com/AP/wire_detail.php?wire_num=60967

[[Return to top](#)]

Food Sector

18. *January 17, Minneapolis Star Tribune* — **Three Minnesota school districts to consider irradiated lunches. Three Minnesota school districts will be the first in the state, and possibly the nation, to consider using irradiated ground beef supplied by the federal government in school meals.** The first irradiated burger could be served as early as this coming fall in the Spring Lake Park, Sauk Rapids and Willmar districts, Minnesota education officials said Thursday. Before that happens, officials said they will launch community awareness projects about irradiation's role in preventing foodborne diseases, such as that caused by E.coli bacteria. **A recent change in federal regulations allows beef bought by the U.S. Department of Agriculture for the school lunch program to be irradiated.** Some individual schools in Minnesota and other states may use irradiated meat bought through private suppliers, although that is not a widespread practice. But, state school lunch officials said, this is the first time beef bought by the federal government for the school lunch program will be irradiated and served to students.

Source: <http://www.startribune.com/stories/1592/3597221.html>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

19. *January 17, HealthNews.co* — **Test for plague "could combat bioterrorism".** Researchers from France and Madagascar have developed a test for plague that could help save lives in the event of a bioterrorist attack. The scientists say the test can determine whether a person has plague before the illness reaches a terminal stage. **A rapid diagnosis of bubonic and pneumonic plague is essential because the disease is fatal if not treated within 24 hours of onset.** The findings are of particular significance amid concerns that the flea-borne disease – which originates in rodents – could be used in a biological terrorist attack. The researchers developed their diagnostic test using conjugated gold particles to detect antigens of plague bacteria. **The test detected antigens at low concentrations within 15 minutes of a person becoming infected and was 100 per cent reliable.** Dr Suzanne Chanteau, one of the study authors, explains, "We have shown that with this test, the rapid and cost-effective diagnosis of bubonic and pneumonic plague could easily be achieved by health workers in remote sites." In an accompanying commentary, U.S. researchers from National Center for Infectious Diseases in Colorado describe the study that discovered the diagnostic test as "remarkable". The test will soon be available in plague-endemic areas worldwide. **The researchers say that the technique "is expected to fill an important need in bioterrorism preparedness and response".**

Source: <http://www.health-news.co.uk/showstory.asp?id=104958>

20. *January 17, Washington Post* — **Unions call for delay of smallpox vaccine program.** Two of the nation's largest unions have called for a suspension of smallpox vaccination of health care workers until provision is made for medical screening of volunteers and compensation for anyone injured by the vaccine. Jerome M. Hauer, acting assistant secretary for public health and emergency preparedness, said he will continue to look for ways to address safety and compensation issues but will not postpone the program. "There are many people out there who have told us they want to be vaccinated," he said. "We are going ahead with the program." The administration and Congress have provided liability protections for makers of the vaccine as well as hospitals and medical personnel administering it. If, for instance, a hospital patient is accidentally infected with the live vaccine, neither the hospital nor its staff would be responsible for damages. Under provisions of the Homeland Security Act, people injured by the vaccine would have to sue the federal government and prove negligence to be compensated.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A3654-2003Jan16.htm>

[\[Return to top\]](#)

Government Sector

21. *January 17, Associated Press* — **Ridge approved for homeland security post.** The nation faces a long struggle against terrorists, Tom Ridge told a Senate panel that on Friday swiftly approved his nomination to head the new Homeland Security Department. **Ridge spoke of the "enormity of our task" of bringing together 22 federal agencies with 170,000 employees to lead the security campaign.** The new department, he told the Senate Governmental Affairs Committee, "will not in and of itself be able to stop all attempts by those who wish to do us harm." **The committee voted unanimously to approve Ridge, a former congressman and governor of Pennsylvania who since the Sept. 11, 2001, attacks has been President Bush's chief adviser on homeland security. Full Senate confirmation was expected to come quickly so Ridge would be in place when the department is officially established next week.**

Source: http://news.yahoo.com/news?tmpl=story2p/20030117/ap_on_go_co/homeland_security_ridge

22. *January 17, New York Times* — **U.S. expands list of nations whose visitors must register.** The Justice Department yesterday expanded a registration program for visitors, most of them from Muslim and Arab nations, **to include men from Bangladesh, Egypt, Indonesia, Jordan and Kuwait. At the same time, officials said men from 18 of the 20 nations already on the list who failed to meet previous registration deadlines would have extra time to report to Immigration and Naturalization Service offices around the country.** Visitors from those nations who fail to register are subject to deportation. Typically, the registration process entails submitting to fingerprinting, a criminal background check and questions on finances and employment.

Source: <http://www.nytimes.com/2003/01/17/politics/17IMMI.html>

23. *January 17, Washington Times* — **Al Qaeda suspects nabbed by use of cave prints.** Two law-enforcement authorities said. The two men are among 330 aliens apprehended at the border since September as presumed law-enforcement threats, **as part of a federal program known as the National Security Entry-Exit Registration System** – a fingerprinting system that matches foreign visitors against databases of known criminals and terrorists. It was not clear yesterday where the men were detained or where they are being held. **The U.S. military, during risky and often time-consuming searches, destroyed scores of al Qaeda and Taliban caves, confiscated tons of arms and ammunition, and found dossiers with photographs, papers containing the fingerprints of various individuals, computers, tape recordings, instruction manuals and receipts. American soldiers, assisted by federal law-enforcement authorities, lifted what was described at the time as "a great number" of latent fingerprints from papers found in the caves, and others seized in abandoned hideouts and training camps for al Qaeda and Taliban members.** The prints were added to the National Security Entry-Exit Registration System for screening incoming aliens.

Source: <http://www.washtimes.com/national/20030117-311448.htm>

[[Return to top](#)]

Emergency Services Sector

24. *January 17, Washington Post* — **U.S. police officials visit 'epicenter of terrorism'.** Israel has been struggling in recent years to defend itself against suicide bombings that have killed scores of people on buses, in restaurants and in other crowded public places. **So this week 33 senior law enforcement officials from the United States and Canada -- including D.C. Police Chief Charles H. Ramsey, U.S. Capitol Police Chief Terrance W. Gainer and top FBI officials -- came here to learn how authorities deal with the violence and the public's reaction to it.** "It is the epicenter of terrorism, and we're learning how to apply what the Israelis have learned, based on their experiences," said Van. A. Harp, head of the FBI's Washington Field Office, who is among those attending a four-day law enforcement conference. "To me, it has magnified the need for leadership and cooperation and partnership, and the importance of getting information out -- not only so law enforcement can react quickly and effectively, but so the community can, too," Harp said. **For Shlomo Aharonishky, Israeli National Police inspector general and host of the conference, those are some of the main elements of good anti-terrorist police work. "I call your civilian population a strategic asset in the fight against terror," he said. In Israel, he said, public awareness and cooperation are critical tools in thwarting attacks.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A3353-2003Jan16.htm>

[[Return to top](#)]

Information and Telecommunications Sector

25. *January 17, Government Computer News* — **Ridge pledges data merger between agencies.** In his nomination hearing today before the Senate Governmental Affairs Committee, Homeland Security secretary-designate Tom Ridge pledged to blend the government's immigration and law enforcement databases. Ridge said **Congress had given his department the task of merging information gathered by the Immigration and Naturalization Service with that of the FBI and CIA.** "We recognize that we have plenty of information, but we have been unable--not necessarily unwilling--to connect that information," he said. "One of our highest priorities will be to connect those databases." Ridge said Homeland Security officials have identified "a way ahead" in the data fusion task using commercial applications. Ridge said he expects biometric authentication to be a significant part of the department's workload. **"Ultimately there needs to be an international standard" for biometrics, he said. "I can envision a day in the not too distant future that we'll require biometric identification of people crossing the border, and our friends and allies will require that, too."** Ridge said Defense Department secretary Donald Rumsfeld has commissioned a team of specialists to work on homeland systems interoperability, as have FBI director Robert S. Mueller III and CIA director George Tenet. **"That collaboration is with an eye to creating an architecture to make information available across agency lines," he said. "We are not trying to design a brand-new system."**

Source: http://www.gcn.com/vol1_no1/daily-updates/20891-1.html

26. *January 17, Federal Computer Week* — **Davis: IT to see 15 percent boost.** Rep. Tom Davis, (R-Va.), the newly named chairman of the House Government Reform Committee, said Jan. 16 that the Bush administration wants to increase the federal information technology budget by about 15 percent in fiscal 2004. **The president's budget will be officially released Feb. 3, but Davis said it is likely that the budget will focus on using IT to increase security and**

information gathering to thwart terrorist threats. The IT budget request will likely to be about 15 percent more than the baseline fiscal 2002 budget that included \$45 billion for IT, he said.

Source: <http://www.fcw.com/fcw/articles/2003/0113/web-davis-01-17-03.asp>

27. *January 16, CNET News* — **Military worried about Web leaks.** Department of Defense (DOD) Secretary Donald Rumsfeld warned in a directive sent to military units this week that **too much unclassified but worrisome material was popping up on the Web, and said al Qaeda and other foes were sure to take advantage of it.** The directive, drafted as the U.S. is readying troops for a possible attack on Iraq, reminded military Webmasters they must adhere to the department's 1998 policy which says: **"A DOD Web site may not post For Official Use Only information, or information not specifically cleared and approved for public release unless it employs adequate security and access controls."** Rumsfeld's order further restricts what information will be publicly available on military sites, effectively tightening controls that have been in place for at least five years and that became far more strict after the terrorist attacks on the World Trade Center and the Pentagon. **"An al Qaeda training manual recovered in Afghanistan states: 'Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy,'"** Rumsfeld wrote. "At more than 700 gigabytes, the DOD Web-based data makes a vast, readily available source of information on DOD plans, programs and activities. **One must conclude our enemies access DOD Web sites on a regular basis.**" There have been no confirmed reports about classified information making its way to military sites, but Rumsfeld said he was concerned about other categories he dubbed "sensitive" or "for official use only." Rumsfeld said that 1,500 instances of such public distribution have been spotted in the last year.

Source: <http://news.com.com/2100-1023-981057.html>

28. *January 16, Wireless Data News* — **Nationwide priority wireless access needed in emergencies.** The creation of the Department of Homeland Security (DHS) will apply some urgency to the wireless industry's regard for providing priority wireless access during emergencies to government and law enforcement officials. The **Federal Communications Commission asked U.S. carriers more than a year before September 11, 2001, to voluntarily participate in ensuring that local, state and federal government and emergency services officials could have priority access at times when wireline service could be disrupted and demand for wireless service would soar.** The \$73 million needed by the White House's National Communications Systems (NCS) office in order to fund nationwide priority wireless access was not included in the \$355 billion Department of Defense appropriations Congress approved in October. The NCS is being transferred to the recently created DHS, and expects to be funded next year when Congress enacts appropriations for that agency. **"This problem has dropped between the cracks and we do not have the funding to take priority cell phone service around the country,"** Richard Clarke, chairman of the White House's Critical Infrastructure Protection Board, said recently at the Cellular Telecommunications & Internet Association's Homeland Security Conference in Washington, D.C.

Source: <http://www.telecomweb.com/wirelessdata/feature.htm>

29. *January 16, Boston Globe* — **Discarded hard drives found full of personal data.** In a new article in the engineering journal IEEE Security and Privacy, MIT graduate students Simson

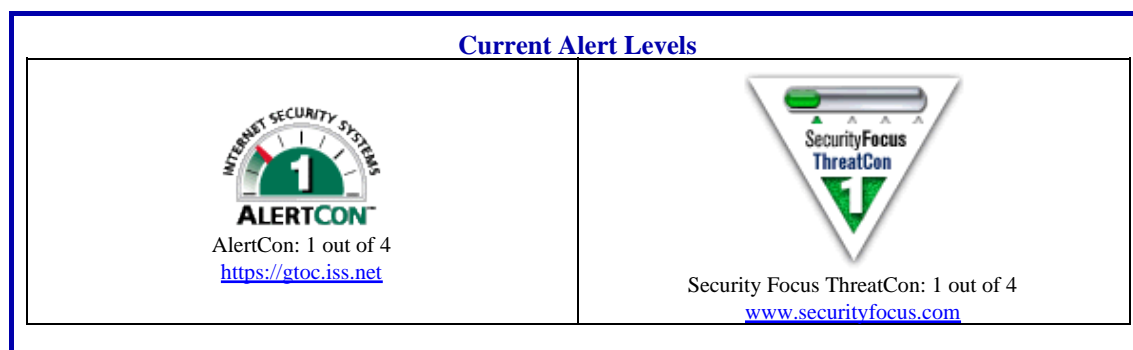
Garfinkel and Abhi Shelat describe how they wondered whether people erased their hard drives before reselling their PCs. The students purchased 158 hard drives at swap meets and used computer shops throughout the United States, and on the Internet auction site eBay. They wound up with 129 drives that actually worked. Then they used commonplace software tools to look for data on the drives. They found sensitive personal information, including 3,700 credit card numbers. Sometimes, **the previous owners had taken the trouble to delete important files, not realizing that a PC's delete function doesn't really remove the data, but conceals it from the computer's operating system. In other cases, the users went further and "reformatted" the hard drive. This process appears to wipe out all data on the disk, but again, the information is still there and can be read using common recovery tools.** They acquired a drive that had been used in an automatic teller machine. There they found account numbers and balances for the bank's customers. **Out of 129 usable drives purchased by Garfinkel and Shelat, only 12 had been properly purged of all data.** This is done with a program that dumps meaningless clumps of randomly chosen digits onto the drive. Such programs are available for free on the Internet, but running them can take several hours for each drive.

Source: http://www.boston.com/dailyglobe2/016/business/Discarded_hard_drives_found_full_of_personal_data+.shtml

30. *January 16, Federal Computer News* — **Net-centric success depends on culture. The future of network-centric warfare will rely just as much on policies and cultural adaptability as it will on the technology on which it runs,** according to a panel of experts assembled at the Armed Forces Communications and Electronics Association's (AFCEA) International West 2003 conference in San Diego January 15. **While new technology will continue to be adopted quickly, the success of network-centric operations will largely depend on how the U.S. forces and their allies use that technology.** Rear Adm. Charles Munns, director of the Navy Marine Corps Intranet, said that network-centricity is happening throughout the Navy. "The intranet we are building is the answer we need to deal with the future. NMCI is going to take 1,000 [local-area networks] and morph them into one interoperable, secure intranet." Others on the panel said **just as much attention needs to be paid to getting technology and standards to allied and coalition forces as is being paid to enhance U.S. forces.** Commodore Jon Welch of Great Britain's Royal Navy said remembering the allies has been an overlooked part of adapting to a network-centric model, and it is one that could cause serious problems in future wars. **"Tell the allies what you're buying and what you're doing with it,"** he said.

Source: <http://www.fcw.com/fcw/articles/2003/0113/web-net-01-16-03.asp>

Internet Alert Dashboard



Current Virus and Port Attacks

Virus:	#1 Virus in the United States: PE_FUNLOVE.4099 Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios–ns), 80 (http), 1433 (ms–sql–s), 4662 (???), 445 (microsoft–ds), 139 (netbios–ssn), 53 (domain), 21 (ftp), 8714 (???), 3389 (ms–term–serv) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[[Return to top](#)]

General Sector

31. *January 20, Reuters* — Antiterror police raid a mosque in London. British antiterrorist police officers raided a London mosque and said the action was linked to the recent discovery of the deadly poison ricin in an apartment here, Scotland Yard said. The mosque is home to one of Britain's most outspoken Muslim clerics. Seven people were arrested under the Terrorism Act 2000, the Scotland Yard police said. **Officers raided the Finsbury Park mosque and two adjacent buildings in north London as part of a planned intelligence operation, the police said.** The London police discovered ricin in an apartment in the nearby Wood Green area of the capital on Jan. 5. The mosque is the base of Sheik Abu Hamza al–Masri, leader of the group Supporters of Shariah, or Islamic law. Sheik Masri has become Britain's most notorious Muslim cleric because of his praise for Al Qaeda, Osama bin Laden's terrorist network, and his outspoken criticism of Western foreign policy. The police did not say whether Sheik Masri was among those arrested.

Source: <http://www.nytimes.com/2003/01/20/international/europe/20MOSQ.htm>

32. *January 16, Platts Global News* — Iran may have bought Pakistan bomb know–how. The Islamic Republic of Iran has obtained design information to develop and construct uranium enrichment gas centrifuges from Pakistan's nuclear program, Western intelligence sources have told Platts. **If the sources are correct, this could be the second country that has bought Pakistani technology applicable to nuclear weapons; intelligence sources earlier alleged Pakistan sold the technology to North Korea.** Sources said that the experts in Pakistan who Western governments believe shared the know–how with Iran had made decisions virtually independently of Pakistan's civilian government during the 1990s, although civilian leaders were apprised of the transactions. Iran has been trying to procure materials needed to build the centrifuges, Western officials said, and it is believed that several years are still needed before Iran can be ready to embark on full–scale uranium enrichment. Centrifuges are a closely guarded technology that can purify uranium so it can be used as a nuclear bomb core. In the late 1980s, Iran restarted its nuclear energy program after years of dormancy following the 1979 revolution. German intelligence reported in the early 1990s suspicions that Iran had tried to purchase centrifuge know–how from Pakistan, which purloined the technology years before from Urenco, a European uranium enricher. **On Feb. 25, inspectors from the UN International Atomic Energy Agency are slated to visit an Iranian site in Natanz which the U.S. alleges is a complex to house a uranium enrichment plant utilizing gas centrifuges.** Diplomatic sources said Iran has identified the project to the IAEA as a future enrichment facility; it is expected inspectors will find only empty structures.

Source: <http://www.platts.com/stories/nuclear3.html>

[\[Return to top\]](#)

NIPC Products & Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web-site (<http://www.nipc.gov>), one can quickly access any of the following NIPC products:

[NIPC Advisories](#) – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

[NIPC Alerts](#) – Alerts address major threat or incident information addressing imminent or in-progress attacks targeting specific national networks or critical infrastructures.

[NIPC Information Bulletins](#) – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

[NIPC CyberNotes](#) – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:

Melissa Conaty (202-324-0354 or mconaty@fbi.gov)

Kerry J. Butterfield (202-324-1131 or kbutterf@mitre.org)

Distribution Information

NIPC Watch and Warning Unit (202-323-3204 or nipc.watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.